SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards.

1. The Company must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.

2. The Company must properly authenticate a Customer using a method appropriate for the information sought prior to disclosing CPNI based on Customer-initiated telephone contact, online account access, or an in-store visit.

   a. Telephone Access to CPNI containing Call Detail Information (CDI). The Company will only disclose Call Detail Information over the telephone, based on Customer-initiated telephone contact, if the Customer first provides the Carrier with a password, as described in Section 10.C.3., that is not prompted by the Carrier asking for Readily Available Biographical Information, or Account Information. If the Customer does not provide a password, or does not wish to create a password, the Company may only disclose Call Detail Information by sending it to the Customer's Address of Record, by calling the Customer at the Telephone Number of Record (rather than using Caller ID), or by providing it in person upon presentation of a Valid Photo ID matching the Customer's Account Information.

   - If the Customer is able to provide Call Detail Information to the Company during a Customer-initiated call without the Company's assistance, then the Telecommunications Carrier is permitted to discuss the Call Detail Information, provided by the Customer (but not other Call Detail Information).

   - If a Customer requests non-Call Detail Information CPNI, the Company need not first obtain a password from the Customer, but must nevertheless authenticate the Customer.

   - The Company need not require Customer to setup a password, but must provide the Customer the option to do so.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards (Cont'd).

b. Online Access to CPNI. The Company must authenticate a Customer without the use of Readily Available Biographical Information, or Account Information, prior to allowing the Customer online access to CPNI related to a Telecommunications Service account. Once authenticated, the Customer may only obtain online access to CPNI related to a Telecommunications Service account through a password, as described in Section 10.C.3., that is not prompted by the Company asking for Readily Available Biographical Information, or Account Information.

- The Company may choose to block access to a Customer's account after repeated unsuccessful attempts to log into that account.

c. In-Office Access to CPNI. The Company may disclose CPNI (including Call Detail Information) to a Customer who, in the Company's office, first presents a Valid Photo ID matching the Customer's Account Information.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards (Cont'd).

3. Establishment of a Password. In order to provide a Customer CPNI containing Call Detail Information, the Company must authenticate the Customer without the use of Readily Available Biographical Information, or Account Information. The Company may establish passwords, among other methods:

   a. At the time of service initiation;

   b. Using a Personal Identification Number (PIN). The Company may supply the Customer with a randomly-generated PIN, not based on Readily Available Biographical Information, or Account Information, which the Customer would then provide to the Carrier prior to establishing a password. The Company may supply the PIN to the Customer by a Company-originated voicemail or text message to the Telephone Number of Record, or by sending it to an Address of Record so as to reasonably ensure that it is delivered to the intended party.

   c. The Company is not required to create new passwords for customers who already have a password, even if the password uses Readily Available Biographical Information. However, the Company must not prompt the Customer for Readily Available Biographical Information, and any back-up authentication method cannot use Readily Available Biographical Information.

4. Establishment of Back-up Authentication Methods. The Company may create a back-up Customer authentication method in the event of a lost or forgotten password. The back-up Customer authentication method may not prompt the Customer for Readily Available Biographical Information, or Account Information. The shared secret is the preferred method for establishing backup authentication.

5. Reauthentication. If a Customer cannot provide the correct password or the correct response for the back-up Customer authentication method, the Customer must establish a new password.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

6. Notification of Account Changes. The Company must notify a Customer *immediately whenever an authentication password*, Customer response to a back-up means of authentication for lost or forgotten passwords, online account, or Address of Record is created or changed.

   a. This notification is not required when the Customer initiates service, including the selection of a password at service initiation.

   b. This notification may be through a Company-originated voicemail or text message to the Telephone Number of Record (not caller ID), or by mail to the Address of Record, and must not reveal the changed information or be sent to the new Account Information.

   c. A change of address should be mailed to the former address, rather than the new address.

7. Business Customer Exemption. The Company may bind itself contractually to authentication regimes other than those described in this Manual for services they provide to business Customers that have both a dedicated account representative and a contract that specifically addresses the Company's protection of CPNI.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

D. Notification of Customer Proprietary Network Information Security Breaches.

1. The Company will take reasonable steps to protect CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.

2. The Company must notify law enforcement of a Breach of its Customers' CPNI. A Breach occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

3. The Company shall not notify its Customers or disclose the Breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement. As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the Breach, the Company shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni. The Company will indicate its desire to notify its Customer or class of Customers immediately concurrent with its notice to the USSS and FBI.

   a. Notwithstanding any state law to the contrary, the Company shall not notify Customers or disclose the Breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in the following Paragraphs b. and c.

   b. If the Company believes that there is an extraordinarily urgent need to notify any class of affected Customers sooner than otherwise allowed under Paragraph a. immediately above, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected Customers only after consultation with the relevant investigating agency. The Company shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such Customer notification.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

D. Notification of Customer Proprietary Network Information Security Breaches *(Cont'd)*.

c. If the relevant investigating agency determines that public disclosure or notice to Customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the Company not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the Company when it appears that public disclosure or notice to affected Customers will no longer impede or compromise a criminal investigation or national security. The agency will provide in writing its initial direction to the Company, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by Carriers.

4. After the Company has completed the process of notifying law enforcement as described in Paragraphs 3.a – 3.c. above, it shall notify Customers of the Breach.

5. Recordkeeping. The Company must maintain a record, electronically or in some other manner, of any Breaches discovered, notifications made to the USSS and the FBI pursuant to the above paragraphs, and notifications made to Customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the Breach, and the circumstances of the Breach. The Company must retain the record for a minimum of 2 years.

APPENDIX 1

ANNUAL CERTIFICATE OF COMPLIANCE WITH CPNI RULES

Including—

FILING INSTRUCTIONS AND ACCOMPANYING COVER LETTER TO THE FCC

Filing Instructions

Attached is a model Certificate of Compliance with the FCC's CPNI rules. It contains blanks for the insertion of Company-specific information. **The certificate must be signed by an officer (i.e., the President, V.P., Secretary) of the Company. Electronic copies of the Certificate and cover letter may be obtained from the Telecommunications Association of Michigan.**

The FCC's revised CPNI rules state that a carrier must file a "compliance certificate" each year that addresses compliance with the FCC's CPNI regulations, along with:

- A "statement accompanying the certificate" to explain how its operating procedures ensure compliance with the FCC's CPNI regulations;
- An explanation of any actions taken against data brokers; and
- A summary of all Customer complaints received in the past year concerning the unauthorized release of CPNI.

The attached Certificate of Compliance addresses these subjects in a single document. Also attached is a sample cover letter to accompany the filing.

This Certificate of Compliance must be filed on or by March 1 each year relating to the prior calendar year.

Simply filing the certificate is not enough. Your Company must make sure that it actually engages in the practices discussed in the Certificate before signing and filing it.

Below are the procedures for filing. **Electronic filing is recommended unless the Certificate contains confidential information on the Company's method of combating pretexting (See Paragraph 16 of the Certificate; consultation with legal counsel is advisable).** Mailed filings are not deemed to be filed until actually received from the FCC (47 CFR 1.7). Thus, paper filings should be mailed several days before they are due.

ELECTRONIC PAPERLESS FILING:

The easiest way to file is electronically through the FCC's Electronic Comment Filing System (ECFS): http://www.fcc.gov/cgb/ecfs/. Put both the cover letter and Certificate in a single PDF. Click on "Submit a Filing" on the right side of the screen. In completing the transmittal screen, filers should include their full name, U.S. Postal Service mailing address, and the proceeding number which is 06-36. Under "Document Type," select "Statement."

Additional electronic copies must go to: Byron McCoy, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, **byron.mccoy@fcc.gov;** and Best Copy and Printing, Inc. (BCPI), **fcc@bcpiweb.com**.

PAPER FILING:

Companies that choose to file by paper must file an original and four copies of each filing. Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Marlene H. Dortch, Office of the Secretary, Federal Communications Commission, 445 12th Street, SW, *Washington, DC 20554.*

Companies can also send their filings using commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail), by sending them to 9300 East Hampton Drive, Capitol Heights, MD 20743.

Additional paper copies must go to: Byron McCoy, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, Room 4-A234, 445 12th Street, S.W., Washington, D.C. 20554, or by email to byron.mccoy@fcc.gov; and Best Copy and Printing, Inc. (BCPI), Portals II, 445 12th Street, S.W., Room CY-B402, Washington, D.C. 20554, (202) 488-5300, or via e-mail to fcc@bcpiweb.com.

[Company Letterhead]

EB Docket No. 06-36

February 4, 2011

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street S.W., Suite TW-A325
Washington, D.C. 20554

RE: **Form 499 Filer ID #802095**

Dear Secretary Dortch,

In accordance with 47 CFR 64.2009(e), please find attached the Company's Annual Compliance Certificate for the previous calendar year, 2010. The Compliance Certificate includes the Company's:

- Statement explaining how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

If you have any questions regarding this filing, please direct them to the undersigned.

Sincerely,

Todd Roesler
Chief Executive Officer
Ace Telephone Association

Enclosure

cc: Byron McCoy, Telecommunications Consumers Division, FCC Enforcement Bureau, byron.mccoy@fcc.gov

Best Copy and Printing, Inc., fcc@bcpiweb.com

CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

Including:

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

Explanation of Any Actions Against Data Brokers, and

Summary of all Customer Complaints Received

Todd Roesler signs this Certificate of Compliance in accordance with § 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and 47 CFR 64.2009, on behalf of Ace Telephone Association (Company), related to the previous calendar year, 2010.

This Certificate of Compliance addresses the requirement of 47 CFR 64.2009 that the Company provide:

- A "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

On Behalf Of The Company, I Certify As Follows:

1. I am the Chief Executive Officer of the Company, and therefore an officer of the Company. My business address is 207 E Cedar Street, Houston MN 55943.

2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to CPNI.

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

3. I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's regulations governing CPNI, including those adopted on March 13, 2007 in CC Docket No. 96-115.

4. The Company ensures that it is in compliance with the FCC's CPNI regulations. The Company trains its personnel regarding when they are authorized to use CPNI, when they are not authorized to use CPNI, and how to safeguard CPNI. The Company maintains a CPNI Compliance Manual in its offices for purposes of training of new and current employees, and as a reference guide for all CPNI issues. Our CPNI Compliance Manual is updated to account for changes in law, including the FCC's most

recent changes to its regulations governing CPNI, adopted on March 13, 2007 in CC Docket No. 96-115. The CPNI Manual contains key all essential information and forms to ensure the Company's compliance with CPNI regulations.

5. The Company has established a system by which the status of a Customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

6. Company personnel make no decisions regarding CPNI without first consulting with management.

7. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.

8. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

9. In deciding whether the contemplated use of the CPNI is proper, management consults one or more of the following: the Company's own compliance manual, the applicable FCC regulations, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval regarding any proposed use of CPNI.

10. Further, management oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the Customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. Management also reviews all notices required by the FCC regulations for compliance therewith. Before soliciting for approval of the use of a Customer's CPNI, the Company will notify the Customer of his or her right to restrict use of, disclosure of, and access to, his or her CPNI.

11. The Company maintains records of Customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

12. The Company complies with all FCC requirements for the safeguarding of CPNI, including use of passwords and authentication methods, and the prevention of access to CPNI (and Call Detail Information in particular) by data brokers or "pre-texters."

13. The Company, on an ongoing basis, reviews changes in law affecting CPNI, and updates and trains company personnel accordingly.

Explanation of Actions Against Data Brokers

14. The Company has not encountered any circumstances requiring it to take any action against a data broker during the year to which this Certificate pertains.

Summary of all Customer Complaints Received

15. The following is a summary of all customer complaints received during the calendar year of 2008 concerning the unauthorized release of CPNI: None.

16. The Company has no knowledge of any attempt by pre-texters to access its Customer's CPNI.

Date: _____

_____

Todd Roesler
Chief Executive Officer
Ace Telephone Association

APPENDIX 2

EMPLOYEE VERIFICATION OF CPNI MANUAL REVIEW

Employee Verification

Employee Name: _____

I have reviewed the Company's Customer Proprietary Network Information Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

_____
Employee Signature

_____
Date

c: personnel file
CPNI file

Return to Human Resources Department

APPENDIX 3

SAMPLE OPT-OUT NOTICE

OPT-OUT NOTICE

Important notice about your account

Federal law allows telephone companies and wireless telecommunications carriers to use, disclose, or permit access to your information as required by law; with your approval; or in providing the service from which your information was obtained.

What is this information?
It is information called Customer Proprietary Network Information (CPNI) and includes the phone numbers called by a consumer, the frequency, duration, and timing of such calls, and any services purchased by the consumer, such as call waiting.

Who can use this information?
Ace Communications Group and Ace Link Telecommunications, Inc. will use this information. However, we will not provide your personal information to unaffiliated third parties for the marketing of third-party products without your consent.

How can Ace use this information?
This information can be used to advise you about innovative communications services or new communications technology and products. We also provide this information to third parties in order to provide certain Ace-offered products and services, such as our long distance service through Onvoy.

Will Ace protect my information?
YES! You have the right, and we have the duty, under federal law, to protect the confidentiality of this information. Therefore, regardless of whether or not you consent to allowing us to continue providing you with marketing and educational mailings, your account information will be treated confidentially.

How does Ace protect my long distance call information?
If you or someone else calls us with questions about your call details, we will only give out the information by:

[1] calling the person back at the phone number listed on the account, or

[2] mailing the information to the billing address on file, or

[3] asking the person for the password that you had already set up for your Ace account. *(The password cannot be something familiar to others such as Social Security numbers, mother's maiden name, birth dates, etc.)*

What action is necessary on my part to show consent?
No action is necessary. If you do not contact us within 30 days and indicate that we may not use the information to continue providing you with marketing and educational mailings, we will continue to do so.

What if I do not consent?
You can contact us using the contact information below and indicate that you are withdrawing your approval of our use of your CPNI. We will not accept verbal requests; they must be written or emailed. After we receive your request, you will not receive targeted marketing information from us.

Denial of approval will not affect the provision of any services to which you subscribe. You may miss the opportunity to learn of new, innovative service proposals, new packaging that could reduce your monthly bill, or new lower rates on services such as long distance. You will still receive monthly bill inserts, quarterly newsletters, and other publications that are sent to all customers at the same time to keep you up to date on what is happening at Ace.

If I consent, can I change my mind?
YES. You can contact us at any time. Until you do so, your consent is valid.

Contact information:
Ace Communications Group.
PO Box 360
Houston, MN 55943
email: info@acegroup.cc

[Note to Company: Please consult Section 7.E. of CPNI Compliance Manual for when Opt-Out Notices are permissible.]

APPENDIX 4

SAMPLE FORM FOR DISCLOSURE OF CPNI TO THIRD PARTY ON CUSTOMER'S REQUEST

ACE Communications Group

ACELink Telecommunications, Inc.

Authorization Form

Current customer name: _____

Address: _____

City/state/zip: _____

Customer number or telephone number(s): _____

I am the customer of Ace Communications Group or Ace Link Telecommunications, Inc. (Ace) for telecommunications services under the account identified above and request and authorize Ace to disclose to the Authorized Person(s) identified below, upon request by the Authorized Person, all details regarding my account to which I have access, and to make changes to my account.

I agree this authorization will remain valid until Ace receives written notice from me revoking or changing the authorization.

Current customer signature (*must be notarized*): _____

Date: _____

(*Add Remove*) Authorized Person: _____ Contact number: _____

(*Add Remove*) Authorized Person: _____ Contact number: _____

(*Add Remove*) Authorized Person: _____ Contact number: _____

(*Add Remove*) Authorized Person: _____ Contact number: _____

4-digit password must be created: _____ _____ _____ _____

(Authorized Person(s) will need to know this password to access the account.)

Subscribed and affirmed before me in the County of _____, State of _____, this _____ day of _____, 20____.

_____

Notary's official signature

_____

Commission expiration date

APPENDIX 5

Log of Customer Complaints Related to CPNI

LOG OF CUSTOMER COMPLAINTS RELATED TO CPNI

Affected Customer Name	Date of Complaint	Description of Complaint

APPENDIX 6

Section 222 of the Communications Act

Available upon request from Administration

APPENDIX 7

FCC CPNI Rules

Available upon request from Administration

Red Flags Compliance Manual and Operating Procedures

For

Ace Telephone Association
Ace Telephone Company of Michigan, Inc.
Ace Link Telecommunications, Inc.
Allendale Telephone Company
Drenthe Telephone and Communications

February 4, 2011

TABLE OF CONTENTS

SECTION 1

DEFINITIONS

Account: A continuing relationship established by a person with a Creditor (like the Company) to obtain a product or service for personal, family, household or business purposes, and includes the provision of services on a deferred payment basis.

Annual Report: See Section 9.

Board of Directors: The Company's board of directors.

Covered Account: An Account that the Company offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. Telecommunication service accounts can be Covered Accounts. The term also includes any other Account for which there is a reasonably foreseeable risk to Customers or to the Company of Identity Theft, including financial, operational, compliance, reputation, or litigation risks (See Section 4).

Company: Ace Telephone Association, Ace Telephone Company of Michigan, Inc., Ace Link Telecommunications, Inc.; Allendale Telephone Company; and Drenthe Telephone and Communications.

SECTION 1

DEFINITIONS (CONT'D)

Consumer Report: A written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's identity which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for service to be used primarily for personal, family, or household purposes, employment purposes, or any other purpose authorized under 47 USC 1681 *et seq.*

Credit: The right granted by a Creditor, like the Company, to defer payment of debt or to incur debts and defer its payment or to purchase property or services on a deferred payment basis.

Creditor: A person, like the Company, who regularly extends, renews, or continues Credit, or who regularly arranges for the extension, renewal, or continuation of Credit, or any assignee of an original Creditor who participates in the decision to extend, renew, or continue Credit. Telecommunication service providers can be Creditors.

Customer: A person that has a Covered Account with a Creditor or a financial institution.

Identity Theft: A fraud committed or attempted using the Identifying Information of another person without authority.

SECTION 1

DEFINITIONS (CONT'D)

Identifying Information: A name or number that may be used, alone or in conjunction with any other information, to identify a specific person. The following are examples of Identifying Information:

- Name, Birth Date, Social Security Number, Drivers License or Identification, Alien Registration, Passport Number, Employer or Tax Identification Number;
- Unique Biometric Data, such as a Fingerprint, Voiceprint, Retina or Iris Image, or other Physical Representation;
- Unique Electronic Identification, Address, Routing Code.

Notice of Address Discrepancy: A notice from a consumer reporting agency informing the Company of a substantial difference between the address that the consumer provided and the address in the agency's file for the consumer.

Red Flag: See Section 3.

Readily Available Biographical Information: Information drawn from the Customer's life history and includes such things as the Customer's social security number (or the last four digits), mother's maiden name, home address, or date of birth.

Service Provider: A provider of a service directly to a financial institution or Creditor.

SECTION 2

STATEMENT OF CORPORATE POLICY

The policy of Ace Telephone Association, Ace Telephone Company of Michigan, Inc., Ace Link Telecommunications, Inc.; Allendale Telephone Company; and Drenthe Telephone and Communications (the Company) is to comply with the letter and spirit of all laws of the United States, including those pertaining to Identity Theft contained in the Fair Credit Reporting Act, as amended, 15 USC 1681 *et seq.*, and the Federal Trade Commission's (FTC's) regulations, 16 CFR Part 681. The Company's policy is to protect against the risk of Identity Theft.

The FTC's regulations require the Company to establish a written Identity Theft Prevention Program, and to train its personnel accordingly. This Manual, in conjunction with the Company's Customer Proprietary Network Information (CPNI) Manual, constitutes the Company's written Identity Theft Prevention Program.

All personnel are required to follow the policies and procedures specified in this Manual.

- Any questions regarding compliance with applicable law and this Manual should be referred to Todd Roesler, 507-896-6292; or Heather Benson, 507-896-6276.
- The following individuals are responsible for oversight of the Company's Identity Theft Prevention Program:
  Todd Roesler, 507-896-6292
  Heather Benson, 507-896-6276
- The Company's Board of Directors Approved this Manual on April 29, 2009.

SECTION 3

WHAT IS A RED FLAG?

A Red Flag is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Examples of Red Flags:

- Alerts, notifications, or warnings from consumer reporting agencies, law enforcement, Customers, or victims of Identity Theft.
- Presentation of suspicious documents or personal identification information
- Unusual use or suspicious activity related to a Covered Account.

The purpose of this Manual is to set forth the Company's policies and procedures regarding Red Flags and the prevention and mitigation of Identity Theft.

SECTION 4

IDENTIFICATION OF COVERED ACCOUNTS

The Red Flag rules require the Company to periodically determine whether it offers or maintains Covered Accounts.

The Company will treat all Accounts involving the provision of service on a deferred-payment basis to the public (including residential and business services), as Covered Accounts. A business customer is defined as an end-user of services which is not a governmental or public entity.

The Company will, on an ongoing basis, determine whether any Accounts that it has not previously treated as Covered Accounts, should be treated as Covered Accounts.

SECTION 5

OVERVIEW OF IDENTITY THEFT PREVENTION PROGRAM

The Company endeavors to detect, prevent and mitigate Identity Theft (1) in connection with the opening of a Covered Account, and (2) with respect to existing Covered Accounts.

The Company will—

1. Identify relevant Red Flags for the Covered Accounts that the Company offers or maintains (see Section 6);

2. Detect Red Flags (see Section 6);

3. Take appropriate action to prevent and mitigate any detected Red Flags (see Section 7); and

4. Periodically update this Manual to reflect changes in risks to Customers and to the safety and soundness of the Company from Identity Theft (see Section 8).

SECTION 6

IDENTIFYING RED FLAGS

OPENING OF NEW ACCOUNTS

The Company has determined that a reasonably foreseeable risk of Identity Theft exists when prospective Customers seek to open new Accounts. The Company will therefore use reasonable measures to identify a person or entity that seeks to open a Covered Account.

This Section 6 therefore identifies Red Flags applicable to the opening of new Covered Accounts, and establishes the Company's method of detecting such Red Flags.

The Company will not provide any service for a Covered Account until it is able to reasonably identify the prospective Customer in accordance with this Section 6. If the Company detects a Red Flag during the process of opening a Covered Account, it will place the provision of service on hold until it can satisfactorily resolve the Red Flag.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Covered Accounts for Personal, Family or Household Purposes.

1. Required Information: When a prospective Customer seeks to open a Covered Account for residential service (i.e., for personal, family or household purposes), the Company will ask for the following from the prospective Customer(s) listed on the Covered Account:

   - name;
   - address;
   - birth date;
   - social security number
   - an unexpired government-issued identification bearing a photograph, such as a driver's license or passport, if the Customer is at the business office to open the account.

   The Company will also encourage (but not require) Customers to establish passwords as a means of protecting against potential future Identity Theft.

   The Company will encourage Customers who establish passwords not to use Readily Identifiable Biographical Information.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Accounts for Personal, Family or Household Purposes (Cont'd).

2. Identification Confirmation.

a. The Company will order a Consumer Report as a tool to confirm identity and will confirm the following:

- the name, social security number and birth date provided by the prospective Customer match
- the prospective Customer is confirmed to be age 18 or older

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Accounts for Personal, Family or Household Purposes (Cont'd).

2. Identification Confirmation (Cont'd).

b. If the prospective Customer is in the business office, the Company will inspect the prospective Customer's identification for any signs of falsification, such as:

- misspellings
- a photo that does not resemble the prospective Customer
- inconsistencies in color, texture or images (such as erasures or smudges)
- raised edges around a photograph indicating the placement of a second photograph over an original photograph
- card wear inconsistent with date of issuance (such as an identification that appears new but bears an issuance date of many years)

c. The Company will create a record of the means used to verify a Customer's identity. The Company will retain such record until 5 years after the Account is closed. Upon disposal, the Company will completely destroy the record.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

B. Opening of Business Accounts.

For a prospective business Customer, the Company will require documents to verify the existence of the business before providing service. Such documents may include:

- Articles of Incorporation or Articles of Limited Liability Company
- Partnership agreement

Partnerships using social security numbers and sole proprietorships may use the personal information of the sole proprietor or partners.

A business customer is defined as an end-user of services which is not a governmental or public entity.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

C. Examples of Red Flags in the Opening of New Accounts.

1. Alerts, notifications or warnings from consumer reporting agencies, law enforcement, Customers, Company employees, or victims of Identity Theft.

   a. Company employee has personal knowledge that prospective Customer is using a false identity.

   b. Consumer report contains a fraud or identity theft alert.

   c. Consumer report reveals that the name, social security and birth date of prospective Customer don't match.

   d. Consumer report reveals that the prospective Customer is not age 18 or older.

   e. Consumer report reveals that social security number is associated with a deceased person.

   f. The Company receives notice from a Customer, a victim of Identity Theft, law enforcement, or any other person that the Company may have opened an Account for a person engaged in Identity Theft.

2. Suspicious Documents and Personal Identifying Information.

   a. Information on the identification is inconsistent with information provided by the person opening a new Covered Account.

   b. The person presenting the identification doesn't look like the photo or match the physical description.

   c. Documentation that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

C. Examples of Red Flags in the Opening of New Accounts (Cont'd).

3. Unusual Use of, or Suspicious Activity Related to, the Covered Account.

a. A Customer advises of unauthorized charges or transactions in connection with a Covered Account, excluding charges commonly disputed in the telecommunications industry such as long distance calls, pay-per-view and video-on-demand purchases, service call charges, and reconnect charges. These charges are typically customer-initiated from their home or relate to work the Company does on-site so there is little risk of identity theft.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

PROTECTION OF EXISTING ACCOUNTS

The Company has policies and procedures in place to safeguard customer proprietary network information (CPNI). The Company will continue to utilize its CPNI policies procedures as a safeguard against unauthorized access to Customer CPNI, including pre-texting. Pre-texting is the practice of obtaining call record detail and other CPNI under false pretenses. The Company also monitors suspicious transactions, and verifies change of address requests in accordance with its CPNI Compliance Manual.

The Company updates its Manual to account for changes in law, and it contains all essential information and forms to ensure the Company's compliance with CPNI regulations.

The Company will continue to follow its CPNI Compliance Manual as a means of preventing Identity Theft. The Company will also continue to improve its Identity Theft Prevention Program based on its experience with past incidents of Identity Theft, and new methods of committing Identity Theft of which it becomes aware.

The Company treats the following as Red Flags—

- Alerts, notifications, or other warnings from consumer reporting agencies or Service Providers;
- Suspicious address changes;
- The unusual use of, or other suspicious activity related to, a covered Account; and
- Notice from Customers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with a Covered Account.

SECTION 7

PREVENTING AND MITIGATING IDENTITY THEFT

The Company will respond appropriately when it detects a Red Flag. In determining how to respond, the Company will consider aggravating factors that may heighten the risk of Identity Theft.

Appropriate responses include one or more of the following depending on the circumstances:

- Monitoring a Covered Account;
- Placing the provision of service on hold until it the Red Flag can satisfactorily be resolved;
- Requiring the Customer to come to the business office to present an unexpired government-issued identification bearing a photograph, such as a driver's license or passport;
- Adding a "Red Flag" warning on a Covered Account;
- Contacting the Customer;
- Reopening a Covered Account with a new account number;
- Declining to open a Covered Account for a prospective Customer;
- Closing an existing Covered Account (in accordance with state regulatory rules, if applicable);
- Not collecting on a Covered Account; or
- Notifying law enforcement (see CPNI Compliance Manual).

SECTION 8

UPDATING THE IDENTITY THEFT PREVENTION PROGRAM

The Company will update this Program periodically to reflect changes in risks to Customers or to the safety and soundness of the Company from Identity Theft.

In updating this Program, the Company will consider the following:

- The Company's experiences with Identity Theft.
- Changes in methods with which Identity Theft is committed.
- Changes in methods to detect, prevent, and mitigate Identity Theft.
- Changes in the types of Accounts that the Company offers or maintains.
- Changes in the Company's business arrangements, such as mergers, acquisitions, alliances, joint ventures, and Service Provider arrangements.

SECTION 9

ANNUAL REPORT

The Company will designate a person to be responsible for preparing an Annual Report to the Board of Directors, appropriate committee of the Board, or a designated senior-level manager.

The Annual Report will address at least the following:

- The effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts.
- The effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft with respect to existing Covered Accounts.
- Arrangements with Service Providers.
- Significant incidents involving Identity Theft and management's response.
- Recommendations for material changes to the Company's Identity Theft Prevention Program.

The Annual Report will be in a format similar to that contained in Appendix 1.

SECTION 10

SERVICE PROVIDERS

To the extent that the Company engages a Service Provider to perform an activity *in connection with one or more Covered Accounts, the Company will ensure that the* Service Provider has its own Identity Theft Prevention Program to detect and address Red Flags.

The Company is ultimately responsible for complying with Red Flag rules even if it outsources Account-related activity to a Service Provider.

SECTION 11

USE OF CONSUMER REPORTS

To the extent that the Company uses Consumer Reports in the opening of a new Covered Account, it will comply with this Section 11.

The Company will do one or more of the following to determine whether it has a reasonable belief that the Consumer Report relates to the prospective Customer about whom it has requested the report:

- Compare the information in the Consumer Report with information the Company uses to verify the prospective Customer's identity as outlined in Section 6.
- Compare the information in the Consumer Report provided by the consumer reporting agency with information the Company obtains from third-party sources.
- Verify with the prospective Customer.

The Company will not consider a Notice of Address Discrepancy as a Red Flag due to the nature of the telecommunications industry where services are provided at an immovable physical location. Prospective customers opening accounts are typically moving to a new address that would not yet be on file with a Consumer Reporting agency.

SECTION 12

DISCIPLINARY ACTION

Any failure to follow this Manual will result in appropriate disciplinary action in accordance with established Company disciplinary policies. Such failures shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. The Company will also require additional training to ensure future compliance.

APPENDIX 1

ANNUAL REPORT FORM

To be completed by the Board of Directors, appropriate committee of the Board of Directors, or a designated senior-level manager.

ANNUAL REPORT FOR _____

This Annual Report constitutes _____ Company's (Company) obligation under the Federal Trade Commission's (FTC) regulations and guidelines, 16 CFR Part 681, to produce an Annual Report to address the Company's compliance with the FTC's Red Flag regulations.

1. Effectiveness of Policies and Procedures

a. Opening of Covered Accounts

The Company provides the following report regarding the effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts:

b. Existing Covered Accounts

The Company provides the following report regarding the effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with existing Covered Accounts:

2. Arrangements with Service Providers

The Company [does/does not] outsource some services to third party Service Providers related to Covered Accounts. [If the Company "does," list them and state:] The Company has taken the following measures to ensure that its Service Provider(s) have Identity Theft Prevention Program(s) to detect and address Red Flags:

3. Significant Incidents Involving Identity Theft

The Company reports the following significant incidents involving Identity Theft and management's response:

4. Recommendations for Material Changes to the Program

The Company should consider the following changes to its Identity Theft Prevention Program.

_____
[Typed Name]
[Typed Title]
Dated: _____

APPENDIX 2

EMPLOYEE VERIFICATION OF RED FLAG COMPLIANCE MANUAL REVIEW

Employee Verification

Employee Name: _____

I have reviewed the Company's Red Flag Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

_____
Employee Signature

_____
Date

c: personnel file

LINE 610

ACE TELEPHONE ASSOCIATION

STUDY AREA CODE

351346

Study Area Name: Ace Telephone Association

Study Area Code: 351346, 361346

Program Year: 2014

Contact: Cynthia Sweet, 507-896-6211, csweet@acecomgroup.com

Certification that the carrier is able to function in emergency situations

Ace Telephone Association (Carrier) is able to remain functional in an emergency situation through the use of back-up power to ensure functionality without an external power source. Carrier has backup battery reserve in its central office, which enables it to provide service for a minimum of 8 hours. Carrier's service is consistent with requirements and the obligations to provide service in emergency situations as set forth in § 54.202(a)(2).

Carrier's network is engineered to provide maximum capacity in order to handle excess traffic in the event of traffic spikes resulting from emergency situations. Carrier has redundancy in its network for use in re-rerouting traffic when facilities are damaged.

LINE 3026

ACE TELEPHONE ASSOCIATION

STUDY AREA CODE

351346

PUBLIC DOCUMENT – TRADE SECRET DATA HAS BEEN EXCISED

(3005a) Operating Report for Privately-Held Rate of Return Carriers		FCC Form 481	
Balance Sheet - Data Collection Form		OMB Control No. 3060-0986	
Page 1 of 3		July 2013	
<010>	Study Area Code	<010>	351346
<015>	Study Area Name	<015>	Ace Telephone Association
<020>	Program Year	<020>	2014
<030>	Contact Name - Person USAC should contact regarding this data	<030>	Cynthia Sweet
<035>	Contact Telephone Number - Number of person identified in data line <030>	<035>	507 896 6211
<039>	Contact Telephone Email Address - Email Address of person identified in data line <030>	<039>	csweet@acecomgroup.com
	☐ Files as reviewed single company		☑ Filed as audited single company
	☐ Filed as reviewed consolidated company		☐ Filed as audited consolidated company
	☐ Filed as subsidiary of reviewed consolidated company		☐ Filed as subsidiary of audited consolidated company

CERTIFICATION

We hereby certify that the entries in this report are in accordance with the accounts and other records of the system and reflect the status of the system to the best of our knowledge and belief.

Signature Date

PART A. BALANCE SHEET

	ASSETS	BALANCE PRIOR YEAR	BALANCE END OF PERIOD
CURRENT ASSETS			
1.	Cash and Equivalents		
2.	Cash-RUS Construction Fund		
3.	Affiliates:		
	a. Telecom, Accounts Receivable		
	b. Other Accounts Receivable		
	c. Notes Receivable		
4.	Non-Affiliates:		
	a. Telecom, Accounts Receivable		
	b. Other Accounts Receivable		
	c. Notes Receivable		
5.	Interest and Dividends Receivable		
6.	Material-Regulated		
7.	Material-Nonregulated		
8.	Prepayments		
9.	Other Current Assets		
10.	Total Current Assets (1 Thru 9)		
NONCURRENT ASSETS			
11.	Investment in Affiliated Companies		
	a. Rural Development		
	b. Nonrural Development		
12.	Other Investments		
	a. Rural Development		
	b. Nonrural Development		
13.	Nonregulated Investments		
14.	Other Noncurrent Assets		
15.	Deferred Charges		
16.	Jurisdictional Differences		
17.	Total Noncurrent Assets (11 thru 16)		
PLANT, PROPERTY, AND EQUIPMENT			
18.	Telecom, Plant-in-Service		
19.	Property Held for Future Use		
20.	Plant Under Construction		
21.	Plant Adj., Nonop. Plant & Goodwill		
22.	Less Accumulated Depreciation		
23.	Net Plant (18 thru 21 less 22)		
24.	**TOTAL ASSETS (10+17+23)**		

	LIABILTIES AND STOCKHOLDERS' EQUITY	BALANCE PRIOR YEAR	BALANCE END OF PERIOD
CURRENT LIABILITIES			
25.	Accounts Payable		
26.	Notes Payable		
27.	Advance Billings and Payments		
28.	Customer Deposits		
29.	Current Mat. L/T Debt		
30.	Current Mat. L/T Debt-Rur. Dev.		
31.	Current Mat.-Capital Leases		
32.	Income Taxes Accrued		
33.	Other Taxes Accrued		
34.	Other Current Liabilities		
35.	Total Current Liabilities (25 thru 34)		
LONG-TERM DEBT			
36.	Funded Debt-RUS Notes		
37.	Funded Debt-RTB Notes		
	Funded Debt-FFB Notes		
	Funded Debt-Other		
40.	Funded Debt-Rural Develop. Loan		
41.	Premium (Discount) on L/T Debt		
42.	Reacquired Debt		
43.	Obligations Under Capital Lease		
44.	Adv. From Affiliated Companies		
45.	Other Long-Term Debt		
46.	Total Long-Term Debt (36 thru 45)		
OTHER LIAB. & DEF. CREDITS			
47.	Other Long-Term Liabilities		
48.	Other Deferred Credits		
49.	Other Jurisdictional Differences		
50.	Total Other Liabilities and Deferred Credits (47 thru 49)		
QUITY			
51.	Cap. Stock Outstanding & Subscribed		
52.	Additional Paid-in-Capital		
53.	Treasury Stock		
54.	Membership and Cap. Certificates		
55.	Other Capital		
56.	Patronage Capital Credits		
57.	Retained Earnings or Margins		
58.	Total Equity (51 thru 57)		
59.	**TOTAL LIABILITIES AND EQUITY (35+46+50+58)**		

PUBLIC DOCUMENT – TRADE SECRET DATA HAS BEEN EXCISED

(3005b) Operating Report for Privately-Held Rate of Return Carriers
Balance Sheet - Data Collection Form
Page 2 of 3

FCC Form 481
OMB Control No. 3060-0986
July 2013

<010>	Study Area Code	<010> 351346
<015>	Study Area Name	<015> Ace Telephone Association
<020>	Program Year	<020> 2014
<030>	Contact Name - Person USAC should contact regarding this data	<030> Cynthia Sweet
<035>	Contact Telephone Number - Number of person identified in data line <030>	<035> 507 896 6211
<039>	Contact Telephone Email Address - Email Address of person identified in data line <030>	<039> csweet@acecomgroup.com

PART B. STATEMENTS OF INCOME AND RETAINED EARINGS OR MARGINS			
	ITEM	PRIOR YEAR	THIS YEAR
1.	Local Network Services Revenues	[redacted]	[redacted]
2.	Network Access Services Revenues	[redacted]	[redacted]
3.	Long Distance Network Services Revenues	[redacted]	[redacted]
4.	Carrier Billing and Collection Revenues	[redacted]	[redacted]
5.	Miscellaneous Revenues	[redacted]	[redacted]
6.	Uncollectible Revenues	[redacted]	[redacted]
7.	**Net Operating Revenues (1 thru 5 less 6)**		
8.	Plant Specific Operations Expense	[redacted]	[redacted]
9.	Plant Nonspecific Operations Expense (Excluding Depreciation & Amortization)	[redacted]	[redacted]
10.	Depreciation Expense	[redacted]	[redacted]
11.	Amortization Expense	[redacted]	[redacted]
12.	Customer Operations Expense	[redacted]	[redacted]
13.	Corporate Operations Expense	[redacted]	[redacted]
14.	**Total Operating Expenses (8 thru 13)**		
15.	Operating Income or Margins (7 less 14)		
16.	Other Operating Income and Expenses	[redacted]	[redacted]
17.	State and Local Taxes	[redacted]	[redacted]
18.	Federal Income Taxes	[redacted]	[redacted]
19.	Other Taxes	[redacted]	[redacted]
20.	Total Operating Taxes (17+18+19)		
21.	Net Operating Income or Margins (15+16-20)		
22.	Interest on Funded Debt	[redacted]	[redacted]
23.	Interest Expense - Capital Leases	[redacted]	[redacted]
24.	Other Interest Expense	[redacted]	[redacted]
25.	Allowance for Funds Used During Construction	[redacted]	[redacted]
26.	Total Fixed Charges (22+23+24-25)		
27.	Nonoperating Net Income	[redacted]	[redacted]
28.	Extraordinary Items	[redacted]	[redacted]
29.	Jurisdictional Differences	[redacted]	[redacted]
30.	Nonregulated Net Income	[redacted]	[redacted]
31.	Total Net Income or margins (21+27+28+29+30-26)		
32.	Total Taxes Based on Income	[redacted]	[redacted]
33.	Retained Earnings or Margins Beginning-of-Year	[redacted]	[redacted]
34.	Miscellaneous Credits Year-to-Date	[redacted]	[redacted]
35.	Dividends Declared (Common)	[redacted]	[redacted]
36.	Dividends Declared (Preferred)	[redacted]	[redacted]
37.	Other Debits Year-to-Date	[redacted]	[redacted]
38.	Transfers to Patronage Capital	[redacted]	[redacted]
39.	Retained Earnings or Margins end-of-Period [(31+33+34)-(35+36+37+38)]		
40.	Patronage Capital Beginning-of-Year	[redacted]	[redacted]
41.	Transfers to Patronage Capital	[redacted]	[redacted]
42.	Patronage Capital Credits Retired	[redacted]	[redacted]
43.	Patronage Capital End-of-Year (40+41-42)		
44.	Annual Debt Service Payments	[redacted]	
45.	Cash Ratio [(14+20-10-11)/7]		
46.	Operating Accrual Ratio [(14+20+26)/7]		
47.	TIER [(31+26)/26]		
48.	DSCR [(31+26+10+11)/44]		

PUBLIC DOCUMENT – TRADE SECRET DATA HAS BEEN EXCISED

(3005c) Operating Report for Privately-Held Rate of Return Carriers
Balance Sheet - Data Collection Form
Page 3 of 3

FCC Form 481
OMB Control No. 3060-0986
July 2013

<010>	Study Area Code	<010> 351346
<015>	Study Area Name	<015> Ace Telephone Association
<020>	Program Year	<020> 2014
<030>	Contact Name - Person USAC should contact regarding this data	<030> Cynthia Sweet
<035>	Contact Telephone Number - Number of person identified in data line <030>	<035> 507 896 6211
<039>	Contact Telephone Email Address - Email Address of person identified in data line <030>	<039> csweet@acecomgroup.com

	PART C. STATEMENTS OF CASH FLOWS	
1.	**Beginning Cash (Cash and Equivalents plus RUS Construction Fund)**	
	CASH FLOWS FROM OPERATING ACTIVITIES	
2.	**Net Income**	
	Adjustments to Reconcile Net Income to Net Cash Provided by Operating Activities	
3.	Add: Depreciation	
4.	Add: Amortization	
5.	Other (Explain)	
	Changes in Operating Assets and Liabilities	
6.	Decrease/(Increase) in Accounts Receivable	
7.	Decrease/(Increase) in Materials and Inventory	
8.	Decrease/(Increase) in Prepayments and Deferred Charges	
9.	Decrease/(Increase) in Other Current Assets	
10.	Increase/(Decrease) in Accounts Payable	
11.	Increase/(Decrease) in Advance Billings & Payments	
12.	Increase/(Decrease) in Other Current Liabilities	
13.	**Net Cash Provided/(Used) by Operations**	
	CASH FLOWS FROM FINANCING ACTIVITIES	
14.	Decrease/(Increase) in Notes Receivable	
15.	Increase/(Decrease) in Notes Payable	
16.	Increase/(Decrease) in Customer Deposits	
17.	Net Increase/(Decrease) in Long Term Debt (Including Current Maturities)	
18.	Increase/(Decrease) in Other Liabilities & Deferred Credits	
19.	Increase/(Decrease) in Capital Stock, Paid-in Capital, Membership and Capital Certificates & Other Capital	
20.	Less: Payment of Dividends	
21.	Less: Patronage Capital Credits Retired	
22.	Other (Explain) Excise tax refund	
23.	**Net Cash Provided/(Used) by Financing Activities**	
	CASH FLOWS FROM INVESTING ACTIVITIES	
24.	Net Capital Expenditures (Property, Plant & Equipment)	
25.	Other Long-Term Investments	
26.	Other Noncurrent Assets & Jurisdictional Differences	
27.	Other (Explain) salvage, net of cost of removal	
28.	**Net Cash Provided/(Used) by Investing Activities**	
29.	**Net Increase/(Decrease) in Cash**	
30.	**Ending Cash**	